(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 June 2002 (27.06.2002)

PCT

(10) International Publication Number
WO 02/50643 A1

(51) International Patent Classification[7]: G06F 1/00, H04L 9/32

(21) International Application Number: PCT/SE01/02825

(22) International Filing Date:
19 December 2001 (19.12.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/256,672 19 December 2000 (19.12.2000) US

(71) Applicant *(for all designated States except US)*: **CYPAK AB** [SE/SE]; Hamngatan 13, S-111 47 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **EHRENSVÄRD, Jakob** [SE/SE]; Svanvägen 16, S-183 77 Täby (SE).

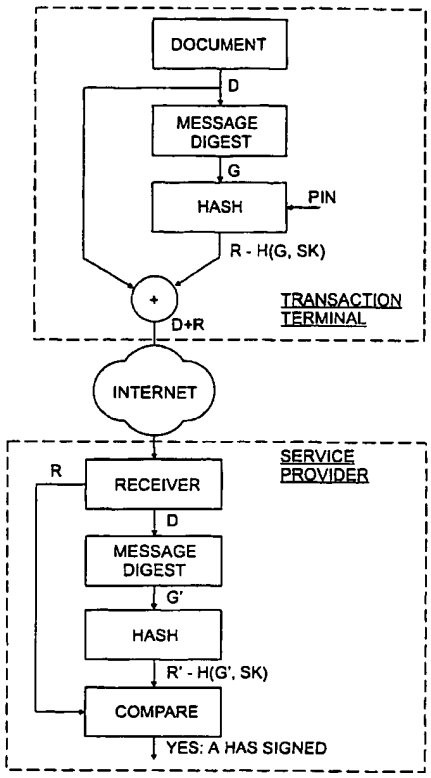
(74) Agent: **LENNEFORS, Stefan**; Stockholms Patentbyrå Zacco AB, Box 23101, S-104 35 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURE DIGITAL SIGNING OF DATA



(57) Abstract: A method of signing digital data. In the method, the data to be signed are subjected to a message digest function to produce a digest of the data to be signed. The message digest is transmitted to a small, mobile transaction device which contains a secret key and a user's PIN code. It is then determined whether a user's PIN code is correct and, if it is, the digest is hashed as a function of said secret key. And the transformed message digest is returned to a service provider. The original data are digested and hashed at the service provider using the same message digest function and secret key. It is finally determined whether the hashed message digest at the service provider matches the hashed message digest received from the transaction device.

WO 02/50643 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SECURE DIGITAL SIGNING OF DATA

Field of the Invention

The present invention relates to a method and a device for performing secure transactions between a service provider such as an institution, a bank, financial institute, retail store, database server, file server etc., and a holder of the device, i.e. transaction requester, which can be a customer or a user of a system.

Background of the Invention

When performing transaction and identification, in a general form (credit cards, club members, fund members, broker contacts, access control etc.) a customer or user identifies itself by supplying a unique person identifier, such as a name, customer number, credit card number, social security number etc. The transaction can either be accepted or require further authentication, such as supplying a secret piece of information such as a password or a PIN(Personal Identification Number)-code. If a lookup in the customer/user file identifies the authentication response as correct, the transaction is considered valid. In the case of authentication, the problem is the fact that the service provider can not verify that the user

is the person he turns out to be.

Several problems arise in terms of security, since this type of processing often is done over "open air", i.e. it can be intercepted and recorded. The fraudulent user can then supply the same identity and authentication and, to the service provider, appear to be the legal user. To supply a credit card number over a phone connection or on a fax-back form is a large discomfort for many users. Furthermore, fraudulent use of personal codes and credit card numbers is a major problem in today's automated world.

The growth of Internet trade has raised several concerns about security when customers have to identify themselves to a remote service provider. There is a general understanding that a severe limiting factor for the public to perform trade and utilize services is the rational fear that confidential information is intercepted during transmission of account numbers and credit card numbers having corresponding passwords or PINs.

There are several methods and devices which address these concerns, including encryption of secure information and Transaction Identification (TID) codes. The latter relates to the issuance of the Service Provider (SP) of a single-use code which is transformed in a non-linear fashion, unique to each user, and then transferred back to the SP. The SP then performs the same non-linear transformation and compares the result returned from the remote location. If the results match, the transaction is considered to be valid.

A common way of performing secure transaction relies on the concept of a Certificate, such as X.509, which is defined as an open standard. The certificate relies on the concept of TIDs and is issued by the SP. The certificate is a piece of information, installed into the software package used to perform transactions, such as an Internet browser. The user

enters additional secret information, such as a PIN Code, which is embedded in te certification process as proof of authenticity.

The certificate method has several drawbacks, the most obvious being that the certificate resides in one computer only. There is no general way of carrying a certificate from computer to computer, or in a more general form, from terminal to terminal. There is also a security drawback involved in the fact that the certificate is stored on a non-removable medium, and can therefore theoretically be opened by someone else using the computer where the certificate is stored.

The fact is that scripting languages, such as Java and VBScript, commonly used to perform a more programmatic behavior of Internet pages, actually can perform fraudulent actions, such as intercepting the PIN-code entered when opening a certificate, copying the certificate information and then transferring the information back to an alien service provider.

Some SPs issue transaction terminals, which are small calculator-like devices including a display, a keyboard, and in some cases a slot for inserting an IC-card with user information. This method solves the problem with mobility, but introduces additional cost for the device. Another drawback of this method is the fact that it is all done manually. To enter a TID, and then collate the processed result back is a time-consuming and error-prone process. The number of digits entered and collated back has to be a compromise between security on one hand, and the convenience of having a short code on the other. It can further be assumed that these manual steps are an obstacle for the customer, which may be one reason not to perform a desired action.

The concept of encryption generally relies on the assumption that the time required to "reverse engineer", i.e. decrypt, the encrypted information is long enough to make it practically impossible to even try to break the encryption scheme. The fabulous growth of both computer processing power and the discovery of new mathematical algorithms have in many cases proven that this assumption is dangerous. Reverse engineering actions, once considered to take several years on the most powerful machine available, can now be performed in minutes by implementation of new algorithms and massive computing power.

Encryption methods, such as Data Encryption Standard (DES), previously known as a hard-to-break schemes are now considered weak. Prime number methods, such as RSA, try to keep ahead of this growth by making longer and longer keys. Fifty-six bit RSA methods are today known to be considerably safe, but some high-security applications rely on 1024 bit numbers. This race of numbers can be expected to continue.

A problem with high-security asymetric encryption schemes is the fact that they usually need heavy numerical processing. By stationary devices, equipped with high-performance microprocessors, such as a PC, this is generally not a major problem. But battery operated, low cost mobile devices, such as cellular phones, portable notebooks etc, generally have limited resources for numerical processing. Embedded applications such as low cost consumer electronics generally have no support for complex operations making this type of processing impractical or even impossible.

The conclusion is that it would be advisable to provide a method and device of addressing these issues and be able to practically prove beyond doubt that a transaction is

secure. Preferably, the scheme should be simple to explain and not rely on the fact that parts of the method must be kept strictly secret.

Moreover, a replacement for a hand-written signature is often required when transmitting digital information. When receiving a digital document wherein the integrity of the received data can be guaranteed, the next challenge is to guarantee the authenticity of the sender.

A common way of performing this task today is to create an authenticable signature of the document, where the receiver can check both the document's integrity and the sender's authenticity. A known method is to use asymmetric encryption, commonly known as Public Key Infrastructure (PKI). First, the information about to be transmitted is passed through a "Message Digest" function, which yields a fixed-length digital signature of the data. Secondly, this digital signature is encrypted using the sender's private key. The encrypted signature is appended to the data being transmitted, where the receiving party can decrypt the received signature and compare it with the expected signature of the received data.

However, the PKI approach exposes several problems, including:

- Encryption key management and safeguarding is difficult to handle, especially for mobile users, where a key is moved between different computers. Also, inexperienced users generally do not understand the importance of careful key management, thereby lowering the overall security level.
- **The key is generally stored in a file and can thereby be compromised without performing a cryptanalytic attack, and moved to an alien, which then is able to impersonate the authentic user.**

- To achieve a reasonable level of security, PKI encryption and decryption is very processing intensive, making it impractical, or even impossible, for usage with low-power, portable devices.

Object of the Invention

An object of the invention is to provide a secure method of signing digital data using a small mobile transaction device similar to a credit card, smart card or the like.

Summary of the Invention

A method of signing digital data comprises the steps of subjecting the data to be signed to a message digest function to produce a digest of the data to be signed, transmitting the message digest to a small mobile electronic transaction device as a challenge signal, hashing the digested signal as a function of a secret key which is stored in the transaction device if the user enters an authentic PIN code to produce a signature, returning the signature with or without the original document to a service provider, and performing at the service provider the same message digest function on the document and the same hash transformation on the digested document as was performed in the transaction device, and determining whether the hashed message digest in the service provider matches the signature received from the transaction terminal.

Brief Description of the Drawings

Fig. 1 is a front view with parts broken away of a transaction card according to the invention;

Fig. 2 is a diagrammatic view showing a transaction card according to Fig.1 in communication with a service provider in a network;

Fig. 3 is a front view with parts broken away of a flat panel having a card transaction terminal embedded in the panel structure;

Fig. 4 shows a first layer printed onto a bottom lamina of a transaction card according to the invention and including capacitive conductor patches;

Fig. 5 shows a second layer printed onto the first layer of the bottom lamina and including an insulating patch;

Fig. 6 shows a third layer printed onto the second layer of the bottom lamina and including electric circuits;

Fig. 7 is a functional diagram of a transaction terminal according to the invention;

Fig. 8 is a functional diagram of a transaction device according to the invention;

Fig. 9 is a block and circuit diagram of a system including a transaction terminal and a transaction device according to the invention; and

Fig. 10 is a flow chart showing how the invention may be used for digital signing.

Description of the Preferred Embodiment

A preferred embodiment of a mobile low-cost electronic transaction device is shown in Figs. 1 through 5.

The transaction device according to the invention is adapted to communicate with a service provider (SP) over a data network, particularly the Internet, via a transaction terminal (TT) having a communication interface such as a card reader (CR). The device has the external shape of a card 10, preferably a credit card, and is optionally provided with a magnetic strip (not shown) and an embossed text field to be allowed for use as a conventional credit card. However, a transaction device according to the invention may have other shapes, for example the shape of a small calculator.

As is apparent from Fig. 1, the card 10 is preferably composed of three laminated sheets 12, 18, 24, preferably of polyester plastics material and having a combined thickness of about 0.8 mm, i.e. the thickness of the conventional credit card.

In the preferred embodiment the card is provided with input means including a keypad 14, data storage and processing means including an integrated circuit (IC) 50, and transceiver/energy supply means including a capacitive transceiver or bi-directional transmitter 38, parts of which are shown in Figs. 6 through 9.

The keypad 14, which is suitably located at an upper part of the card front face has twelve keys for manual entry of numbers 0-9 as well as "Enter" and "Clear" commands. The keypad 14 is preferably a membrane-type keypad which is embedded in the card 10. More precisely, the thin resilient polyester plastic material of the top sheet 12, having printed key symbols on its front face, constitutes the keypad key membranes. On the bottom inside face of

the top sheet 12 electrically conductive switch pads 16 are printed. The intermediate sheet 18 functions as a spacing layer having circular recesses 20 in register with the switch pads 16 and also having a rectangular recess 22 housing IC 50. The bottom sheet 24 has an uppermost printed circuit layer 26 (se also Fig. 4) including switch areas 28 in register with the switch pads 16 and the circular recesses 20. The arrangement is such that when a cardholder presses a key on the keypad 14, the corresponding conductive switch pad 16 overbridges the space of about 0.2 mm formed by the corresponding recess 22 and comes into contact with a registering switch area 28. A corresponding electric circuit 32, which is normally broken by a dense pattern of conductors 30 camming into each other in the switch area 28, is thereby closed. Each electric circuit 32 is connected to the IC 50 via printed connector patches of a connecting interface 54.

As mentioned above, the printed circuit layer 26 forms a top layer in the bottom sheet 24. As indicated in Figs. 5 and 6, the inside of the bottom sheet 24 has two underlying additional printed layers, namely a printed electrically insulating intermediate layer 34 and a printed capacitive bottom layer 36. The bottom layer 36, which forms a part of the capacitive transceiver 38 (Fig. 9) to be later described, comprises three capacitive patches 40, 42, 44 which are electrically connected to the IC 50 via printed connector patches 46, 47, 48. These are in turn connected to connector patches 56, 58, 58 of the connecting interface 54 (Fig. 4) when the top circuit layer 26 is printed onto the insulating intermediate layer 34.

In a manner well known in the art, the IC 50 has data storage, processing and input/output means designed for the particular purpose and for use of the card as a transaction device. Particularly, the storage means is capable of storing therein a Personal Identification

code (PIN) of typically four digits and a Secret Key (SK) of a considerably length. The PIN and the SK which preferably are already stored in the memory when the card is issued to the holder can by no means be retrieved from the card 10. The SK is programmed one time only into the card by the card issuer. In a manner well known 'per se in the art of microelectronics, software and/or hardware means are adapted to prevent readout and altering of the PIN and the SK. The PIN may, however, optionally be altered once from a pre-programmed initial value by the holder before using the transaction card 10.

Fig. 2 shows a transaction card 10 ready for use, placed on a Card Interface (CI) comprising a capacitive close proximity transceiver in the shape of a card reader 60 by a cable 66.

The card reader 60 has a card-receiving surface 62 onto which the card 60 is placed on validating a transaction with a Service Provider (SP) 72 communicating with the card reader via a network 70 and a Transaction Terminal (TT) 68 connected to the card reader 60. The shown card reader 60 has also an alphanumeric display 64 for prompting necessary actions during a transaction process.

As the transaction device according to the invention is independent of an external keypad, the card reader circuitry can be embedded behind a flat surface 62, as illustrated in Fig. 3. For example, the surface 62, can be a hygienic easy to-clean glass counter top surface in a store. In that case, the electrically conducting circuitry, including the capacitive areas, can be almost invisibly applied, for example on an inner surface of a glass sheet lamina, by deposition of an Indium-Tin Oxide (ITO) circuit pattern. The flat surface 62,

can also be a vertical panel face of a rugged outdoor structure which is unsusceptible to occasional vandalism.

The, SP 72 is a bank, Internet store, retail store etc. The SP 72 keeps a record in database 74 of all customers valid to perform transactions.

The TT 68 is a stationary device, connected to the SP via a network. The connection can either be continuous or intermittent. The TT 68 can either be specially designed for the purpose or be a standard personal computer.

The transceiver of the card reader 60 is capable of bidirectional communication with cards. The card reader 60 is shown as a stand-alone device but can also be an integral part (not shown) of the TT 68.

The card can perform data exchange with the TT using the CI/card reader 60. As mentioned above, in the preferred embodiment said data exchange is performed by wireless means using close-proximity capacitive data transmission and power supply for the card.

Figs. 7 and 8 show diagrammatic, functional arrangements of respectively a card reader 60 and the card/transaction device 10, whereas Fig. 9 shows specific components of the combined system..

As indicated in Fig. 9, the capacitive patches 40, 42, 44 of the card 10 will come into registration with corresponding capacitive patches 40b, 42b, 44b facing the patches 40, 42, 44 in close proximity when the card 10 is located on the receiving surface 62 (Fig. 2). The card 10 and the card reader 60 will then form the capacitive circuitry shown in Fig. 9

which is capable of supplying electric power to the circuitry of the card 10 and exchanging digital data between the card 10 and the card reader 60 as follows:

In the following description the card reader is regarded as an external host unit 60 sharing a capactive interface in close proximity to the card 10 regarded as a guest unit and including the integrated circuit 50 connected via an interface 126. The three pairs of conductive areas 40-40b, 42-42b, and 44-44b form the common capacitive interface.

The transaction terminal 68, which can be a standard personal computer, is typically equipped with a V.24/V.28 interface as a standard. The transaction terminal 68 is equipped with a proprietary software driver (not shown) to control the data flow for the host unit 60. Depending on the desired functionality, this driver can either be an installed driver module or a part of an application program.

The CCITT V.24/V.28 electrical specification states a minimum voltage output swing at a stated loading. Even though the specification itself does not state that an attached device may be powered from the interface, as long as the stated maximum loading is not exceeded, it is a benefit to be independent of external power. Where it is undesired to put further loading on the serial port or the serial port itself does not fully comply to the driver requirements stated in the specification, external power may be applied from an AC/DC adapter or batteries included in the host unit. If desired, an interface control signal may be used to control the power of the host unit 60, where one state is a low-power, standby condition and the other an active, full-power state.

A principal circuitry of the host unit 60 may be implemented as follows:

The host unit 60 is designed to be connected to a standard V.24/V.28 serial port, where the voltage levels of outputs RTS and DTR are programmed by the interface software to be at a high level, thereby providing a positive supply voltage for the circuit elements. The Receive Data Input (RxD) has mark level at a negative level, thereby providing a negative supply for a level shifter 98. Additional tank and smoothing capacitors 82, 96 are provided and may be supplemented with a voltage-stabilizing element, such as a parallel zener diode (not shown).

A level shifter 84 provides shifting of input voltages to the host unit, and provides a logic high output when the input is at mark level, i.e. inactive. An oscillator schmitt-trigger NAND circuit 86 will then oscillate at a frequency primarily set by a LC resonant circuit comprising a resistor 90, an inductance 92, and a capacitor 94 present on the output of schmitt-trigger 88. This resonant circuit provides a carrier output on conducting area 42b. By the resistive feedback this design provides for an automatic tuning of the resonant circuit to operate at its peak output amplitude, relatively independent of the complex impedance loading of 42b. By selecting a CMOS/HCMOS schmitt-trigger 88, the value of resistive feedback can be kept high to reduce the loading of the resonant circuit. Further benefits of using HCMOS devices includes low operating power, low output impedance, rail-torail output swing and input protection diodes, thereby providing a high output swing of the resonant circuit with a minimum of design complexity.

When a space level is present on the input of level shifter 84, a logic low output disables the oscillator function, so that the output of the resonant circuit fades and a DC level is present on terminal 42b. When a serial data stream is received on the input of

level shifter 84, the output of the resonant circuit will provide a pulse-modulated carrier, which is then capacitively coupled over to the portable device.

The guest unit 10 has a high input impedance and is further explained below in the detailed description of the transaction device interface.

Accordingly, when capacitive interface plates 40 and 42/44 are placed in close proximity to the corresponding plates 40b, 42b and 44b, capacitors are formed by plates 40-40b, 42-42b and 44-44b. The actual capacitor values are primarily given by the plate size, the distance between the plates and the type of dielectric material(s) present between them.

The design where plates 42 and 44 are connected together implies a reduced stray capacitive coupling between plates 42b and 44b. Another benefit is that the portable device is symmetric, i.e. it can be rotated in steps of 1800 without loss of functionality.

A first closed capacitive loop is formed by following the output of the resonant circuit in the host unit 60, via plates 42b-42 to the guest unit 10, through a rectifier bridge 120 having four diodes 122, through the parallel impedance circuit 114 including a capacitor 116 and a resistor 118, and back to ground in the host unit 60 via plates 40-40b.

A second closed capacitive loop is formed by following the output of the resonant circuit in the host unit 60, via plates 42b-42, 44-44b and via the input diode 106 and resistor 102 down to ground in the host unit 60.

When the oscillator circuit 16 in the host unit 10 is enabled, the first capacitive loop induces a voltage on terminal RX in the guest unit 10. By an optional peak-hold diode and tank capacitor (not shown), a low-current circuitry can then be powered in the guest unit

10, without severely affecting the signal transfer between the host unit 60 and the guest unit 10.

When the oscillator 88 is modulated by a data stream from the transaction terminal 68, a corresponding demodulated output is formed at terminal RX in the guest unit 10. By an optional voltage limiter and schmitt-trigger (not shown) on RX, a clean, demodulated signal can be directly processed by the integrated circuit 50 in the guest unit 10.

The guest unit 10 further comprises a transistor 112 connected in parallel with the impedance circuit 114. Digital data information can be transmitted back from the guest unit 10 to the host unit 60 by controlling the transistor 112 from a TX terminal in the guest unit 10. When the transistor 112 conducts, the input on plate 42 is effectively shorted to ground via plates 40-40b, thereby attenuating the voltage on plate 44 coupled to plate 44b. The quiescent coupling of the carrier filtered in the input network connected to the level shifter 98 in the host unit 60 is then attenuated. A properly selected threshold value of the input to level shifter 98 together with a hysteresis perform the demodulation of the information transferred from the guest unit 10 to the transaction terminal 68.

In the case of power transfer from the host unit 60 to the guest unit 10, it is an undesired effect that NRZ(NonReturn to Zero)-modulated data disable the voltage on the RX terminal in the guest unit. By applying a different modulation scheme well known in the art, such as PPI, FM or Manchester, the off-time can be reduced, thereby enabling a more continuous voltage in the guest unit 10.

This preferred embodiment has an inexpensive, easy to implement, self-tuned design with relaxed requirements of the reactive components. Components having a relatively

poor tolerance of about ±10% of ideal values are usable in the system and are widely available at a low cost. The capacitive loading formed by the guest unit 10 as well as different stray capacitances just slightly moves the oscillator center frequency, without severely affecting the output amplitude.

As the host unit 60 operates at low power, it can be directly powered from the interface signals, thereby eliminating the need for external power, such as provided from an AC adapter or a set of batteries.

The guest unit operates at virtually zero quiescent current, without compromising the abilities to receive data at any time.

Alternatively to the embodiment described above, the card can be designed as a so called Smart Card for communicating data galvanically, i.e. via conductor patches exposed on the front face of the card (not shown) . In that case, and also alternatively in the preferred embodiment described above, the electric energy can be stored in a thin-film battery forming a layer in the card (not shown) . A card having such a self-contained energy source allows the holder to enter the PIN on his own, with less danger of revealing the PIN to others, before the card is placed on the card reader. If the transaction device according to the invention is shaped as a thicker credit-card sized calculator, it can of course have a small conventional cell battery as the electric energy source.

The IC 50 has data processing capabilities to perform a non-reversible transformation using a non-linear function transformation, or hash function, y=h(x,sk) which fulfils the following characteristics:

The output has a fixed output length for any input value of x.

There is no inverse, i.e. x cannot be calculated from a given value of y.

Be simple to calculate in terms of processing power and able to be evaluated by basic integer arithmetics and logical functions, including table lookup.

A device according to the invention is intended to be used in communication with the SP 72 as follows:

The media between the SP 72 and the TT 68 as well as between the TT 68 and the card 10 is considered to be insecure and all information transmitted in any direction can be intercepted and read in clear text by anyone at any time. The embossed card number is considered to have no relationship with an optional credit card number or any other information that may be useful by when intercepted by an alien.

The SP 72 can issue a Transaction Identifier (TID) of a considerable length to the TT 68. The TIDs are issued in a random way that the likelihood of two identical numbers being sent during the lifetime of one single card is extremely small or should must never occur at all.

The card contains a card identity (CID) stored in the IC 50, unique to the cardholder. The CID is considered to be public and may be printed on the card 10 since it is not vulnerable and usable for performing a transaction without the card itself. The CID must have no link to an optional credit card number if it is embossed on the card and recorded in the magnetic strip or CR 60. The CID can be read automatically from the card at any time by the magnetic strip or CR 60.

If desired, the card can provide a signal to the TT 68 for each pressed key on the keyboard 14 to give an audible and/or visible feedback to the user. Said feedback signal has no relation to the key position pressed.

The secret key (SK) stored in the IC 50 can by no means be retrieved from the card in any form and is programmed one time only by the card issuer. Software and/or hardware means prevents readout and altering of the secret key,

As mentioned previously, the card contains a stored Personal Identification Number code (PIN) stored in the IC 50. Said PIN can by no means be retrieved from the card in any form.

The card includes data processing capabilities to perform a non-reversible transformation using a single-use code from the SP via the TT 68 supplied TID and transmit it back to the SP 72 via the TT. Since two identical TIDs should never occur during the lifetime of the card, an alien system cannot perform playback of a recorded response, to thereby allow a fraudulent transaction in the case a previous response is recorded.

To identify a card, the following steps are performed:

1. The TT requests the CID from the card.

2. The card transfers the CID back to the TT. Depending on application, the CID may be transferred back to the SP.

Optionally, the following features can be added, depending on application:

The TT can repetitively request a CID.

When a card is placed on the reader, the application in the TT automatically redirects the user to a preprogrammed application program or URL on the Internet.

Further information about the card can be requested from the SP.

To perform a secure transaction or perform an authentication that the card holder is valid, the following general steps are performed:

1. The TT transmits the CID retrieved as above to the SP.

2. The SP issues a TID that is relayed over to the card via the TT.

3. The cardholder is prompted to enter the PIN.

4. A valid PIN unlocks SK and performs a hash transformation of the TID and SK and transfers the result back to the SP via the TT.

5. The SP performs the same processing as performed in step 4 and compares the retrieved result. If the results match, the transaction is considered to be valid.

To perform another secure transaction, the steps are repeated from step 2.

To further enhance security, the following steps may be followed:

Only one transaction is allowed for each challenge TID received. Each new transaction has to be validated by a new TID.

A timeout is set after a challenge TID is received to the card. A timeout requires a new TID to be issued from the SP.

The card is preprogrammed to perform a preset number of transactions before it gets expired. The card is then permanently blocked for further use by non-reversibly altering a one-time blow memory cell.

The card is preprogrammed with a non-volatile counter, which permanently blocks the card if more than a preprogrammed number of invalid PINs are entered. Said counter is reset each time a valid PIN is entered.

Cards registered as lost and/or stolen gets permanently blocked for further use by the SP issuing a blocking TID, which permanently blocks the card for further use, and, if desired, alerts sales personnel. Said TID is programmed uniquely or randomly for each card and are known only by the SP and in the card, and appears as a normal TID for an alien who intercepts the TID.

Each card may be preprogrammed with a TID sequence map, randomly selected between issued cards, which map allows TIDs with a certain characteristic only. This sequence or scheme must be carefully selected not to cause any undesired effects in the non-linear transformation resulting in a statistically biased response pattern. If a received TID does not match to said scheme, the card immediately gets expired, thus increasing the likelihood of early detection and termination of an alien attempt to issue faked TIDs.

Each card may be programmed to use different transformation algorithms depending on a preprogrammed selection scheme detectable from the TID. The scheme may be preprogrammed into the card and be known only by the SP and in the card.

As mentioned previously, a first-time PIN-code can optionally be initialized by the card holder. The PIN code can then not be altered and is thereafter known by the card holder only.

Since each response from the card requires a complete and validated PIN entry, it is assumed that an alien attempt to provide faked TIDs to the card in order to find out information by the secret key in the card will be unsuccessful. The enhanced security level of blocking the card after a preprogrammed number of transactions further strengthens this assumption.

A statistically proven selection of the key length, a non-linear transformation algorithm and the card expiry counter should make it possible to render this scheme to be unbreakable by all practical means. This further requires a carefully selected randomization scheme to be performed so that no detectable link exists between the CID and the SK or so that no biasing effects occur in the transformation process.

When a customer sends a document to a service provider, it is very often necessary that the service provider know that the document is unchanged and that it has been signed by the customer, i.e. that the sender is who he/she purports to be. The challenge-response scheme described above can be used in the following manner to achieve both objectives.

The main purpose of the card SC is to provide secure authentication of a document using a challenge code (e.g. TID) which is sent by the service provider (SP) to the SC. The SC keypad is used to enter the user's PIN code. If the PIN code is valid (i.e. it matches a reference code stored in the SC non-volatile memory) the challenge is enabled.

According to an additional feature of the invention, this scheme can also be used to establish that a particular customer has signed the document.

For this purpose, the transaction terminal (TT) of the customer (A) includes the capability of performing a message digest (MD) function on the document. The document can be of any arbitrary length. The MD function has the same properties as the hash function described above, the MD output being less than or equal to the length of the input data. The

use of a message digest function is well known. Commonly used MD functions are known as MD2, MD4, MD5, and SHA.

This feature of the invention will be described by referring to a specific example in which a customer A wishes to send a document D (for example, a mortgage loan application) to a service provider (bank B). The process is shown schematically in Figure 10.

The document (which may represent any type of information including drawings, lab data, pictures, etc.) is assumed to be stored in the transaction terminal TT. A Message Digest function is performed on the data in the transaction terminal TT. The message digest function may be MD5 or SHA-1 and produces an output number (digest) G having a fixed length. The digest G is used as a challenge to the card SC. To do this, the customer A enters his/her PIN code using the card keyboard. If the PIN code is the same as the code stored in the SC non-volatile memory, the secret key SK is "unlocked". A hash function is then performed on the message digest G using the secret key SK to produce a digital signature R which is sent to the service provider or bank B with the document D.

B also subjects the document D to the same message digest function to produce a digest G′. B then computes R′ which is the same hash function of G′ and SK (which is known to B). If R = R′, it can be assumed that A has signed the document B.

In the example described above, the document D is returned to the service provider B together with the signature. This is required if the customer A is likely to modify D, for example, by adding data such as an address, etc. to a contract. If the document is not intended to be modified by customer A, then the document can be signed without returning

the document itself to the service provider. The hashed digest (R) is sufficient since the service provider B has the document and, therefore, can perform the same message digest function which, when hashed, yields R'.

The invention also can be used to provide a recorded proven timed trail of the event so that the customer (A) cannot later deny that he or she "signed" the document. To do this, a centrally generated time stamp in the form of a numeric value can be included in the MD function. The time stamp may represent the number of seconds elapsed since a given date.

The foregoing procedure works when at least one of the participants is a "trusted partner" such as a bank which is considered to be well trusted and will not repudiate the document D. Where there is no trusted partner, the procedure may not work because B could fraudulently modify D to create a phantom document D' and then sign D' using the shared key SK. B could then claim that A created D' because the signature is valid.

In such a case, a trusted partner T can be introduced so that the signatures are undeniable. In a two party exchange, this would introduce additional keys Ka and Kb where Ka is shared between A and T and Kb between B and T.

The procedure in this case may be as follows:

1. A transfers document D to T, using the shared key Ka to sign it.
2. T receives D and verifies its authenticity using Ka.
3. T transfers document D to B, using the shared key Kb to sign it.
4. B receives D and verifies its authenticity using Kb.

5. B is confident that only T has Kb and Ka, and trusts T. B therefore is assured that D is authentically signed by A.

In this scenario, B cannot claim that the phantom document D' is signed by A, since T can be consulted to verify the authenticity, as A does not have Ka

Another scenario would probably be more versatile, as it would not require on-line operation with T:

1. A signs document D using Ka and creates a signature Sa, which is appended to the document.
2. A signs the package P (= D + Sa) using the shared key K and creates signature S, thereby assuring the authenticity of both D and Ka.
3. B receives P and verifies S using K.
4. Sa cannot be directly used or verified by B, but is kept as a reference in case of a dispute.

If there is a dispute over the authenticity of D, either A or B may consult T, as T can use Ka to verify the additional signature. A can at any time take any document Dx and sign it using Ka and prove for T that Sa is authentic. Further on, A can always re-sign Dx using Ka, where A can prove for B that B's image of S(Dx, Ka) is identical.

Optionally, the following features can be added, depending on application:

The card may contain a read/write memory area which can be used to store personal information in the card itself, i.e. Internet cookies, user profiles etc. This memory area can be either open to be read at any time or made to request unlocking by a valid PIN-code.

The cardholder may enter further transaction data on the card's keypad, such as transaction amount, available options, secret votes etc.

The CID together with different entries can also be arranged to automatically control a user application environment to connect to a predetermined location, such as an URL of the Internet, a certain home location of a mailbox account etc.

Other advantageous features of the transaction device are:

simple design of reader allows home use, where a personal desktop or palmtop computer can be used as TT with simple Internet downloadable software;

solid state, wireless and sealed design allows for a sealed TT without moving parts or slots;

no degradation due to water, moisture, corrosion, magnetic fields etc.;

capacitive coupling prevents wireless interception of information which is not the case with radio frequency cards available today;

low power design of CI and card; and

low processing power requirements, making it practical for low cost devices which lack support for complex numerical processing.

WHAT IS CLAIMED IS:

1. A method of signing digital data, comprising the steps of:

subjecting the data to be signed to a message digest function to produce a digest of the data to be signed;

transmitting the message digest to a small, mobile transaction device which contains a secret key and a user's PIN code;

determining whether a user's PIN code is correct and, if it is, hashing the digest as a function of said secret key;

returning the transformed message digest to a service provider;

digesting and hashing the original data at the service provider using the same message digest function and secret key; and

determining whether the hashed message digest at the service provider matches the hashed message digest received from the transaction device.

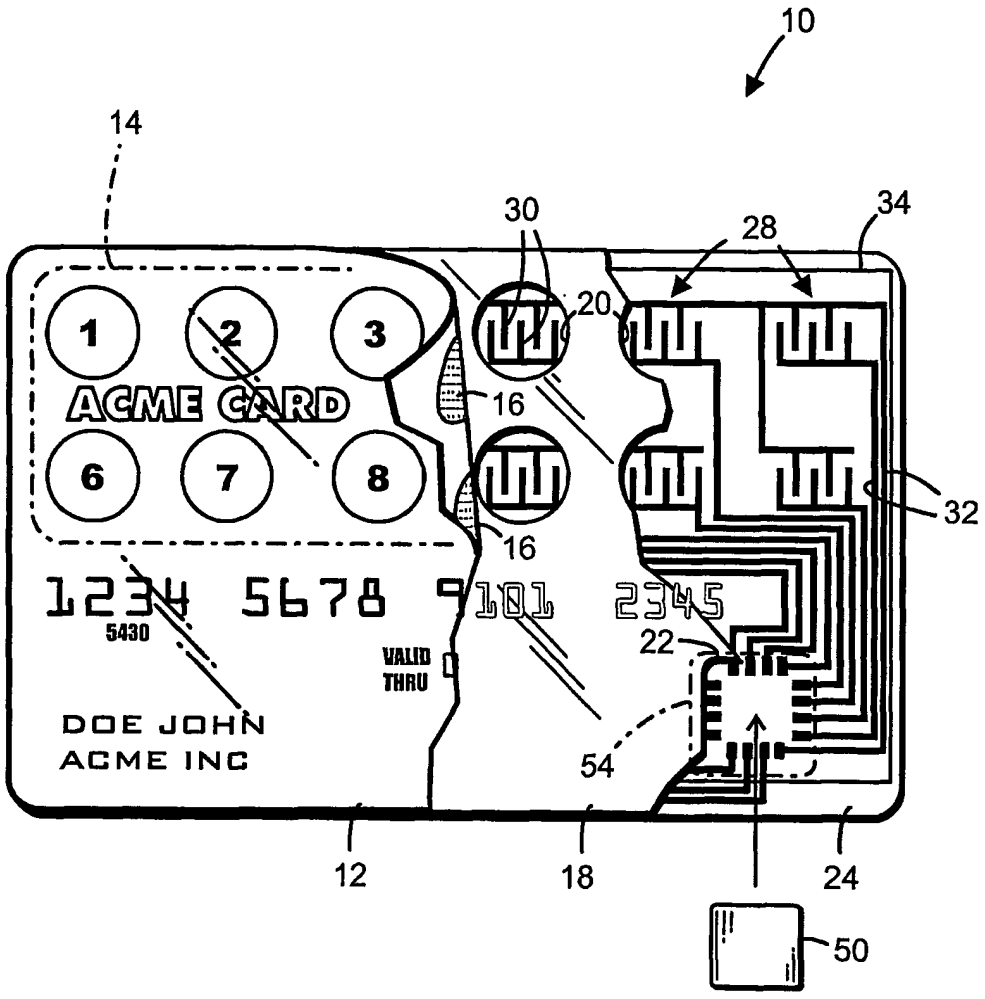

10
14
30
28
34
20
1
2
3
ACME CARD
16
6
7
8
32
16
1234 5678 9101 2345
5430
VALID
THRU
22
DOE JOHN
ACME INC
54
12
18
24
50

Fig. 1

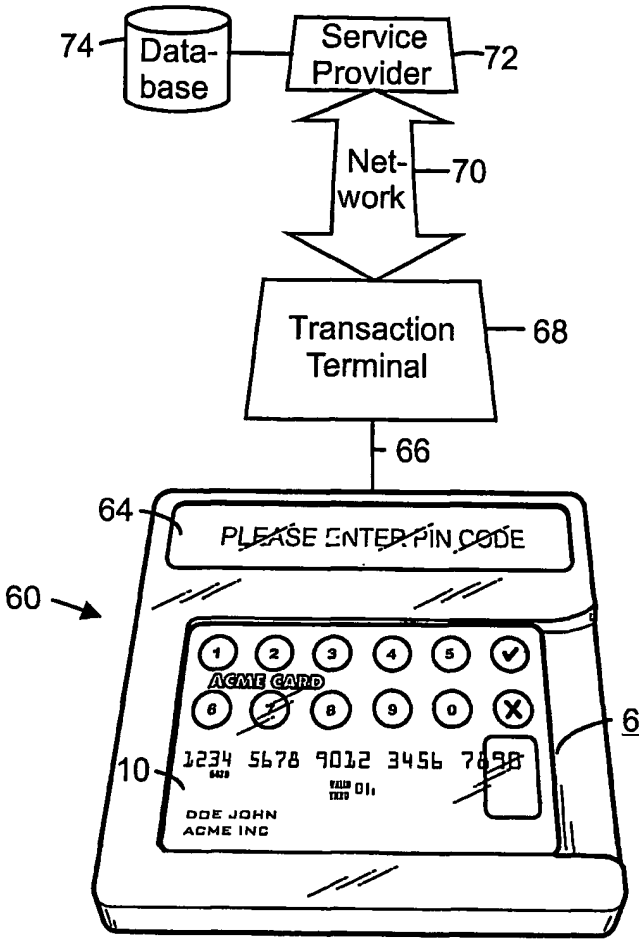

74
Data-base
Service Provider
72
Net-work
70
Transaction Terminal
68
66
64
PLEASE ENTER PIN CODE
60
ACME CARD
62
10
1234 5678 9012 3456 7890
DOE JOHN
ACME INC

Fig. 2

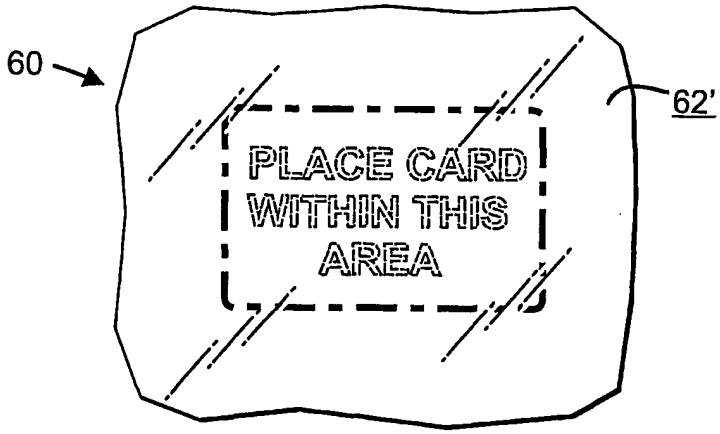

60
62'
PLACE CARD WITHIN THIS AREA

Fig. 3

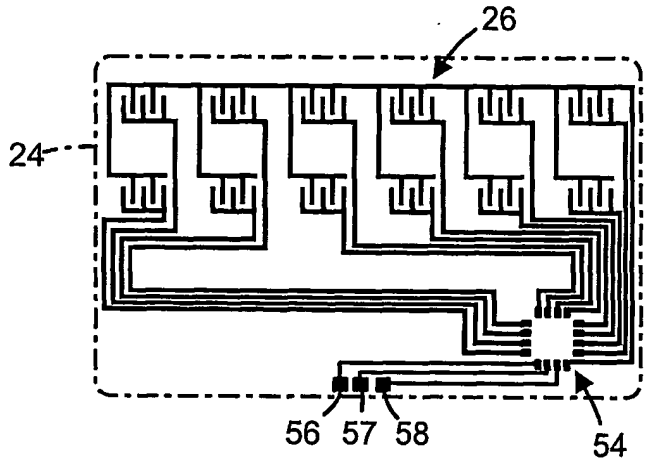


Fig.4

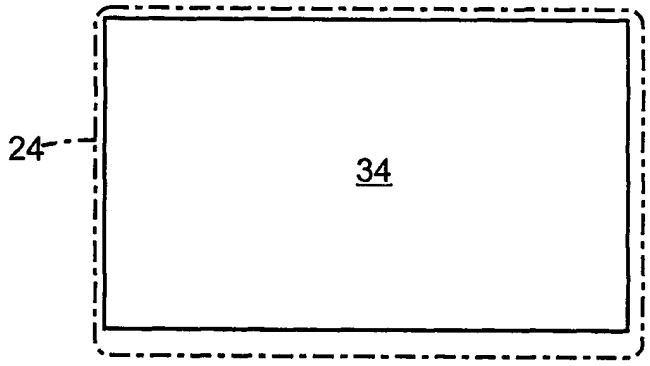


Fig.5

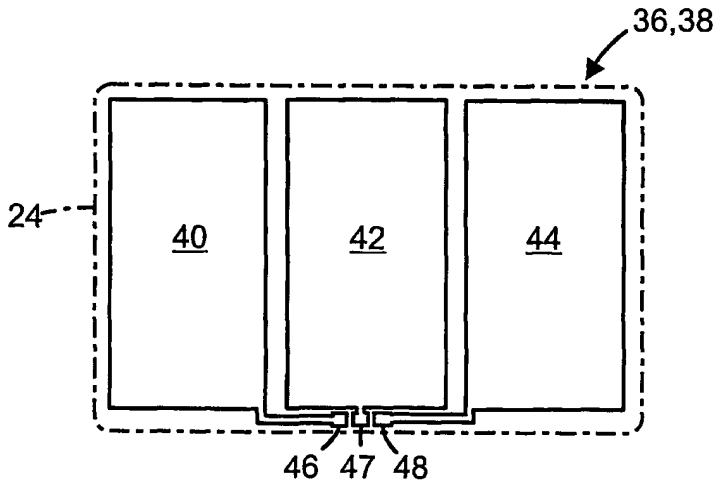


Fig.6

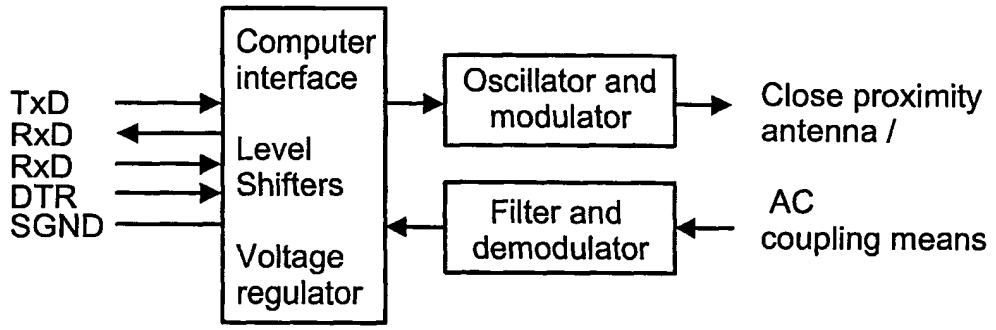

TxD
RxD
RxD
DTR
SGND
Computer interface
Level Shifters
Voltage regulator
Oscillator and modulator
Filter and demodulator
Close proximity antenna /
AC coupling means

Fig. 7

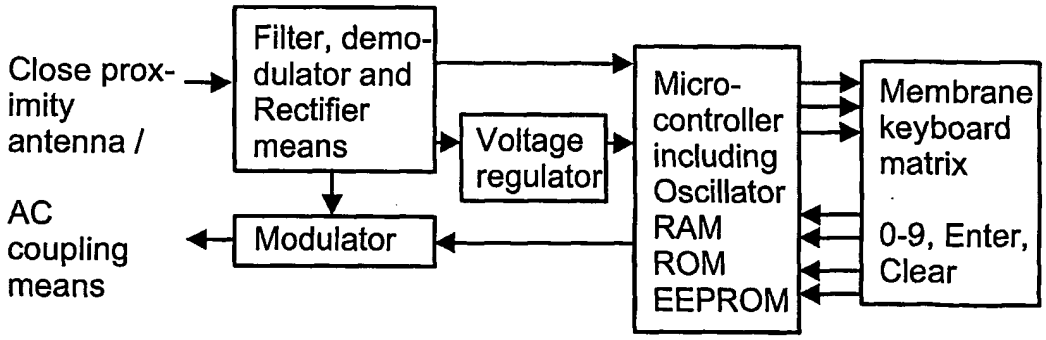

Close proximity antenna /
AC coupling means
Filter, demodulator and Rectifier means
Voltage regulator
Modulator
Micro-controller including Oscillator RAM ROM EEPROM
Membrane keyboard matrix
0-9, Enter, Clear

Fig. 8

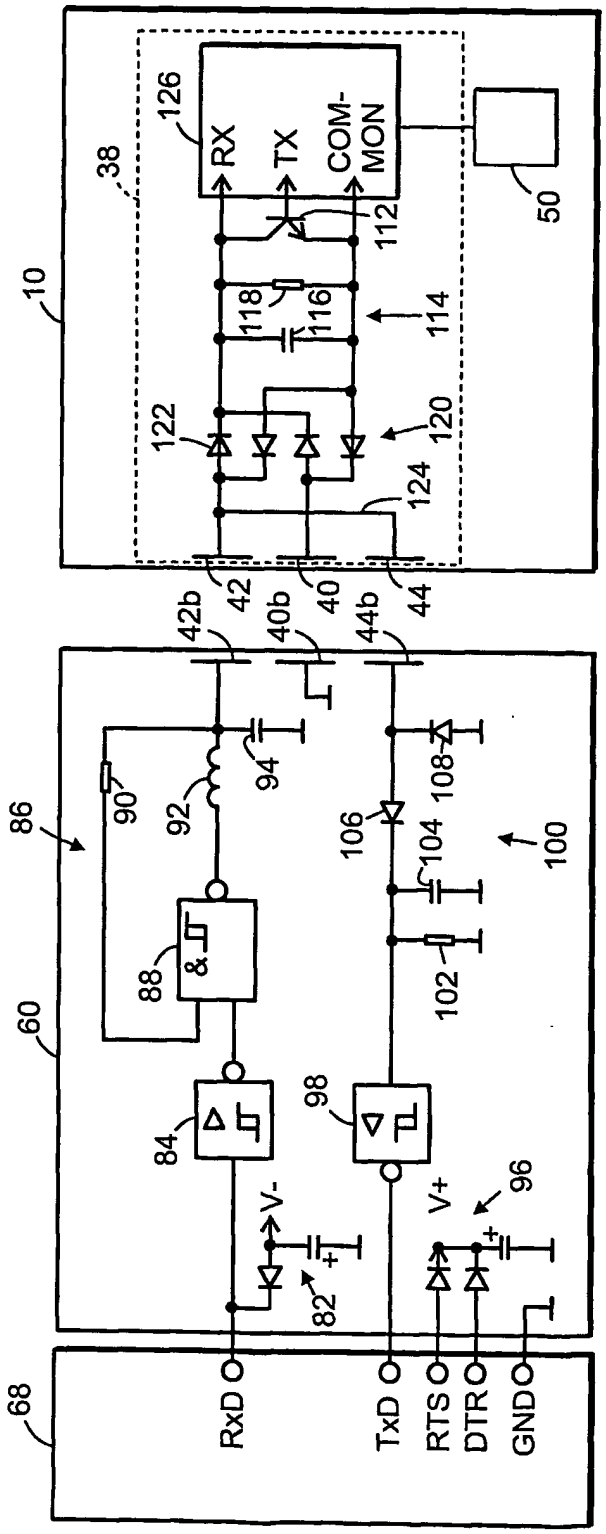

10
38
126
RX
TX
COM-
MON
50
112
118
116
114
122
120
124
42
40
44
42b
40b
44b
86
90
92
94
106
108
104
100
88
102
60
84
98
V-
V+
96
82
68
RxD
TxD
RTS
DTR
GND

Fig. 9

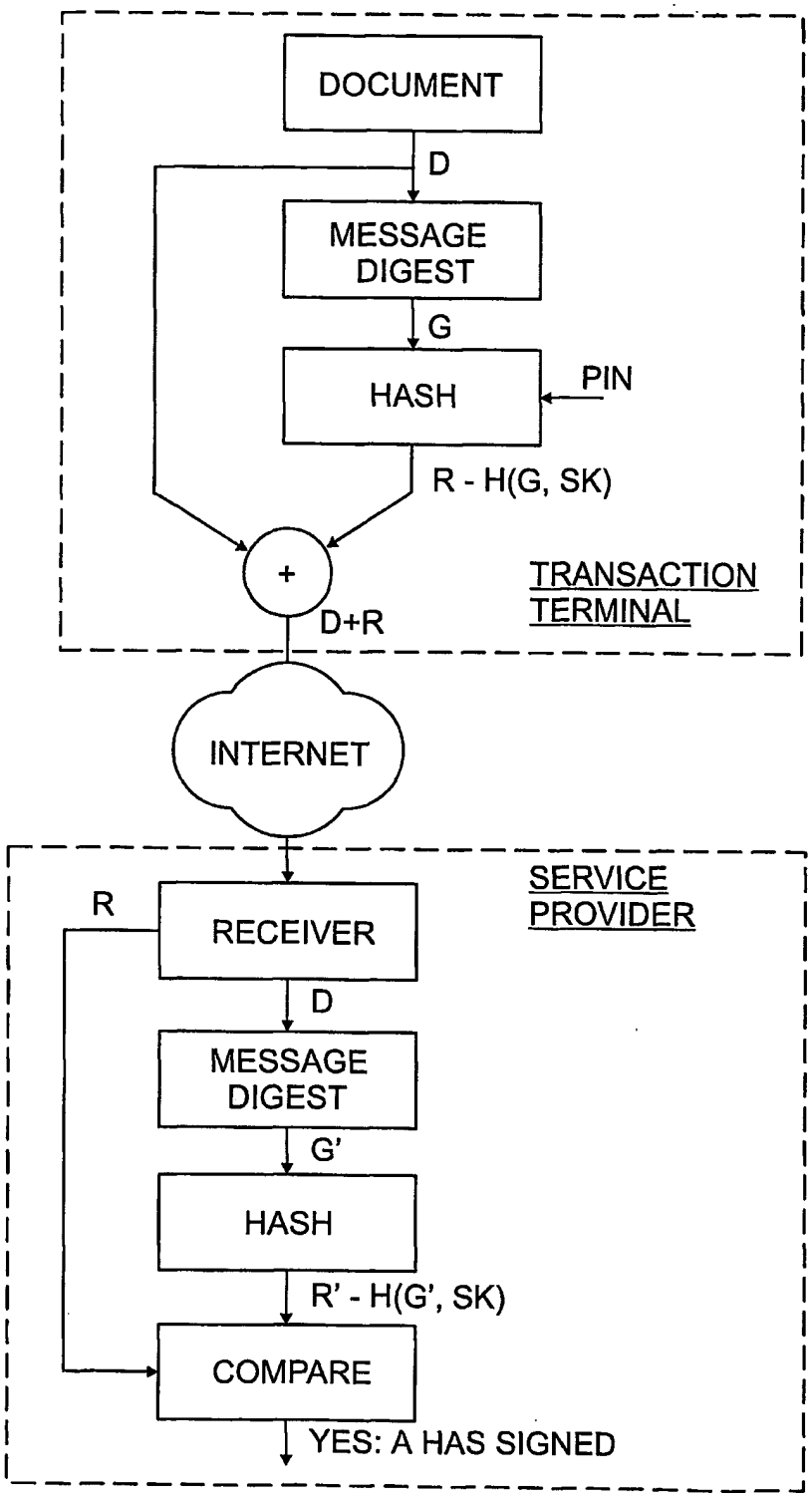

DOCUMENT
D
MESSAGE DIGEST
G
HASH
PIN
R - H(G, SK)
+
D+R
TRANSACTION TERMINAL
INTERNET
SERVICE PROVIDER
R
RECEIVER
D
MESSAGE DIGEST
G'
HASH
R' - H(G', SK)
COMPARE
YES: A HAS SIGNED

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/02825

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 1/00, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F, G06K, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI DATA, EPO INTERNAL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 0042492 A2 (MICROSOFT CORPORATION), 20 July 2000 (20.07.00), abstract --	1
A	US 4453074 A (S.B. WEINSTEIN), 5 June 1984 (05.06.84), see the whole document --	1
A	GB 2275654 A (LANDIS & GYR ENERGY MANAGEMENT (UK) LIMITED), 7 Sept 1994 (07.09.94), see the whole document -- --------	1

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 March 2002	03 -04- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SE 01/02825

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0042492 A2	20/07/00	NONE	
US 4453074 A	05/06/84	AU 565463 B	17/09/87
		AU 1492283 A	29/11/84
		CA 1210470 A	26/08/86
		DE 3319919 A	06/12/84
		FR 2546646 A,B	30/11/84
		GB 2140179 A,B	21/11/84
		GB 8313697 D	00/00/00
GB 3375654 A	07/09/94	NONE	